Buchhaltung Blaschka KG
Friedrich Engels Pl. 15-16/1/10
1200 Wien

Dokumentation

zu den

berufsrechtlichen Vorgaben

in der EU-DSGVO,

im BiBuG 2017,

und im WiEiReG

Version von 2018-01-06

Gerichtsstand: Wien
UID: ATU69352167
Firmenbuch: FN 329864w, HG Wien

Erreichbarkeit:
T: +43 (1) 9346653
M: office@buchhaltung-blaschka.at
W: https://www.buchhaltung-blaschka.at

Bankverbindung:
IBAN: AT773200000010388270
BIC: RLNWATWWXXX

Inhaltsverzeichnis

Kapitel 1

EU-DSGVO

1.1 Vorbemerkungen

Am 25. Mai 2018 wird das Datenschutzgesetz 2000 (DSG 2000) durch die EU-DSGVO (Datenschutz-Grundverordnung) abgelöst. Als EU-Verordnung ist diese unmittelbar - d.h. ohne Umsetzung in nationales Recht - anzuwenden. Die Artikelbezeichnungen beziehen sich - wenn nichts anderes vermerkt ist - auf die DSGVO.

Die Rechtmäßigkeit der Verarbeitung nach den Bestimmungen des DSG 2000 ergibt sich u.a. aus den Standardanwendungen, die in der Liste, im Anhang 1 der StMV (Standard- und Muster-Verordnung), aufgelistet sind.

1.2 Art. 5

Artikel 5 hat die Überschrift "Grundsätze für die Verarbeitung personenbezogener Daten". Auf die genannten Grundsätze

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glaube
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

wird, soweit nötig, im Folgenden eingegangen.

1.3 Art. 6

Die "Rechtmäßigkeit der Verarbeitung" der zu verarbeitenden Daten iSd Abs. 1 lit. a bis f ergibt sich einerseits durch den erteilten Auftrag vom Kunden und andererseits durch rechtliche Vorgaben. Diese ergeben sich vor allem aus Pflichten zum Führen von Aufzeichnungen, die im Abgabenrecht, im Arbeitsrecht sowie im Sozialversicherungsrecht definiert sind.

Durch die Begründung eines Vertragsverhältnisses mit einem Kunden, sind dessen persönliche Daten, als abgabenpflichtige Person, zu verarbeiten (lit. a).

Lit. b kommt zur Anwendung, wenn vor Vertragsabschluß zu prüfen ist, ob in Bezug auf die Bestimmungen der EU-Richtlinie zur Vermeidung von Geldwäsche und Terrorismusfinanzierung[1] die vereinfachte Prüfung angewandt werden darf, oder ob die erhöhten Sorgfaltspflichten anzuwenden sind.

Die lit. c, e und f werden über die bereits oben erwähnten rechtlichen Pflichten, Daten für die Zwecke der Abgabenerhebung zu erfassen, erfüllt. Zusätzlich kommen die Verpflichtungen zur Archivierung der Daten nach beispielsweise folgenden Bestimmungen zur Anwendung: §§ 212 und 216 UGB, §§ 132 und 132a BAO, § 18 Abs. 10 UStG. Für das Arbeitsrecht seien beispielhaft § 8 ArbIG, § 5 ASchG und § 26 AZG genannt. Für das Sozialversicherungsrecht seien exemplarisch die §§ 33 ff ASVG angeführt. Damit werden die Grundsätze der *Rechtmäßigkeit* und der *Zweckbindung* des. Art. 5 erreicht.

Der gesetzliche Auftrag zur Verarbeitung von (personenbezogenen) Daten - iSd lit. e - hat starken Einfluß auf die Erfüllung der Art. 33 ff.

1.4 Art. 9

Die "Verarbeitung besonderer Kategorien personenbezogener Daten" meint die sensiblen Daten iSd DSG 2000.

Auch bisher wurden keine Daten verarbeitet, aus denen die rassische oder ethnische Herkunft, die politische Meinung, die religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit ableitbar sind. Dies entspricht dem Grundsatz der *Datenminimierung* des Art. 5. Derartige Daten werden auch weiterhin nicht verarbeitet werden können, da es in den Speicherstrukturen nicht vorgesehen ist, derartige besondere Kategorien, zu speichern - in Übereinstimmung mit dem Grundsatz der *Speicherbegrenzung* des Art. 5.

1.5 Art. 13

Die "Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person" darf gem. Abs. 4 entfallen, wenn diese Information bereits bei der betroffenen Person vorhanden ist.

[1] siehe Art. 41 und Art. 43 der RL 849/2015/EU

§ 2 ABGB definiert das "Wissen müssen" im österreichischen Rechtsbestand. Von Unternehmern (=Steuerpflichtiger) wird generell verlangt, sich über die einzuhaltende Rechtsmaterie zu erkundigen. Von jedem Dienstnehmer werden persönliche Daten für die Ausstellung des Dienstvertrages und für die Einhaltung der Meldepflichten der §§ 33 ff ASVG verlangt. Somit darf das Vorhandensein dieser Informationen angenommen werden und eine gesonderte Informationspflicht entfällt.

1.6 Art. 14

Die "Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden" betrifft zum einen nur Dienstnehmer des Kunden. Zum anderen entfällt gem. 5 diese Pflicht, wenn (lit. a) die betroffene Person bereits über die Information verfügt, oder (lit. d) die zu verarbeitenden Daten einem Berufsgeheimnis unterliegen und daher vertraulich zu behandeln sind.

§ 39 BiBuG verpflichtet jeden Berufsberechtigten zur Verschwiegenheit, die nach dem Ende des Vertragsverhältnisses fortdauert. Somit kann unter Anwendung des Abs. 5 lit. d diese zusätzliche Informationspflicht entfallen. Lit. a wäre erfüllt, wenn diese Information vom Kunden an seine Dienstnehmer erteilt wird.

Mit der Verschwiegenheitspflicht des § 39 BiBuG - die auch eine Zeugnisentschlagungpflicht enthält - wird der Grundsatz der *Vertraulichkeit* des Art. 5 erfüllt.

1.7 Art. 24

Die "Verantwortung des für die Verarbeitung Verantwortlichen" umfaßt u.a. die beim Art. 25 beschriebenen technischen Maßnahmen bzw. die beim Art. 32 beschriebenen organisatorischen Maßnahmen.

1.8 Art. 25

Der "Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen" wird - obwohl im Prinzip untrennbar, da beides einander bedingt - hier getrennt behandelt. Weiterführenden Details sind als Betriebs- und Geschäftsgeheimnisse klassifiziert, und daher an anderer Stelle dokumentiert.

1.8.1 Security by Design

Zum Datenschutz durch Technikgestaltung gehört u.a. die Verwendung einer privaten Netzwerkadresse[2] für das Intranet. Zugriffe über das Internet - z.B. durch einen VPN-Tunnel - sind weder vorhanden noch geplant. Meldungen wie z.B. diese sind eine (nachträgliche) Bestätigung für diese Designentscheidung. Die Verwendung von WLAN war schon vor dem Bekanntwerden der "KRACK-Attacke[3]" nicht möglich. Trotzdem dieser Beschreibung[4] wird es dabei bleiben.

[2] RFC 1918
[3] abgefragt am 17.10.2017 um 08:07
[4] abgefragt am 20.10.2017 um 07:58

1.8.2 Security by Default

Zum Datenschutz durch datenschutzfreundliche Voreinstellungen muß festgehalten werden, daß Microsoft Produkte "insecure by default" sind. Deswegen kommen - wo möglich - nur mehr Open Source Produkte zum Einsatz[5]. Durch legistische Maßnahmen, wie z.B. den US Patriot Act, der US Behörden vollen Zugriff auf alle Daten gewährt, die sich in einer "Cloud" befinden, wenn der Betreiber ein amerikanisches Unternehmen ist oder einen amerikanischen Eigentümer hat, verbietet den Einsatz jeder Art von Cloud-Lösung von selbst. Dazu gibt es hier ein paar Beispiele.

Aus der langjährigen Erfahrung mit Microsoft-Produkten[6] sei empfohlen *nicht* auf Windows 10 zu migrieren, sondern bei Windows 7 oder Windows 8 zu bleiben. Die Microsoft-Konfiguration von Windows 10 gewährt vom Werk aus, jeder MS App den Vollzugriff auf alle Daten - inklusive aktivierter Geo-Location, aktivierter Kamera-App und aktivierter Mikrofon-App. Während es bei Windows 7 noch vergleichsweise einfach war, die Konfiguration zu finden, um eine datenschutzfreundlichere Einstellung vornehmen zu können, wird mittlerweile bei Windows 10 diese Konfiguration so gut versteckt, daß man explizit wissen muß, mit welchem aufzurufenden Tool eine datenschutzfreundlichere Einstellung erreicht werden kann. Bei Windows 8 sind diese Einstellungen bereits besser versteckt als noch bei Windows 7, aber leichter erreichbar als bei Windows 10.

1.9 Art. 30

Die im Abs. 1 genannten Elemente des "Verzeichnis von Verarbeitungstätigkeiten" sind weitgehend deckungsgleich mit den Angaben bei der jeweiligen Standardanwendung des Anhang 1 der StMV 2004[7] (BGBl II 312 / 2004, zuletzt geändert durch BGBl I 120 / 2017).

Der für die Datenverarbeitung Verantwortliche ist der Komplementär der Buchhaltung Blaschka KG. Der Name und die Kontaktdaten können entweder dem öffentlich einsehbaren Firmenbuch entnommen werden, oder dem Impressum. Mitarbeiter und gegebenenfalls Auftragnehmer unterliegen der Verschwiegenheitspflicht des § 39 BiBuG.

Die nachfolgende Tabelle enthält das Verzeichnis der Verarbeitungstätigkeiten. Die Bezeichnungen wurden von der StMV übernommen.

Code	Bezeichnung
SA001	Rechnungswesen und Logistik
SA002	Personalverwaltung für privatrechtliche Dienstverhältnisse
SA022	Kundenbetreuung und Marketing für eigene Zwecke
SA029	Aktenverwaltung (Büroautomation)
SA037	Melde- und Kontrollsystem zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung

[5] Für die Open Source Community hat Datensicherheit eine sehr hohe Priorität.
[6] von DOS 3.2 bis inklusive Windows 10.
[7] Standard- und Muster-Verordnung nach dem DSG 2000

1.10 Art. 32

Die "Sicherheit der Verarbeitung" soll durch ein Bündel an Maßnahmen erreicht werden. Dazu gehören u.a. die Verwendung einer privaten Netzwerkadresse[8], ein Backup-Konzept und organisatorische Maßnahmen. Zu den organisatorischen Maßnahmen gehört u.a. die Verpflichtungserklärung der Dienstnehmer[9], und speziell die Schaffung von Risikobewußtsein, um beispielsweise nicht jede Mail "blind" zu öffnen. Die Details sind als Betriebs- und Geschäftsgeheimnis klassifiziert und an anderer Stelle dokumentiert.

Aus der Auswertung der anfallenden Daten ist bekannt, daß am SSH-Port in jeder Sekunde bis zu drei parallele Angriffe stattfinden. Beim Mail-Sub-System (Port 25) kommt es im Durchschnitt alle 15 Sekunden zu einem Versuch die Sicherheitsmaßnahmen auszuhebeln. ftp (Port 21) wird mehrmals am Tag mit "Bulk Angriffen" konfrontiert. Der Web-Server liefert jeden Tag rd. 500 MB an Datenvolumen aus. Durch den konsequenten Einsatz von sicherheitsbewußten Open Source-Produkten und der entsprechenden Konfiguration, konnte noch kein gelungener Einbruchsversuch festgestellt werden.

1.11 Art. 33

Die "Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde" wird voraussichtlich unterbleiben können, da nur solche Daten verarbeitet werden, für die es einen gesetzlichen Auftrag gibt. Daher wird es voraussichtlich zu keinem Risiko für die Rechte und Freiheiten natürlicher Personen führen, wenn eine Datenschutzverletzung festgestellt wird.

Sollte eine Verletzung des Datenschutzes festgestellt werden, wird im Einzelfall zu prüfen sein, welche Daten betroffen sind. Davon abgeleitet, kann eine Meldung an die Aufsichtsbehörde zu erstatten sein.

1.12 Art. 34

Die "Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person" wird mit hoher Wahrscheinlichkeit nicht nötig werden, da diese Meldung ein **hohes** Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen als Voraussetzung hat.

Da die Datenverarbeitung auf gesetzlichen Vorgaben basiert, ist es auch nicht möglich, durch diese Datenverarbeitung, in Rechte oder Freiheiten von natürlichen Personen einzugreifen, da dies bereits durch den Gesetzgeber erfolgt ist, der die Verarbeitung der Daten angeordnet hat.

Sollte eine Verletzung des Datenschutzes festgestellt werden, wird im Einzelfall zu prüfen sein, welche Daten betroffen sind. Davon abgeleitet, kann eine Meldung an betroffene natürliche Personen zu erstatten sein.

[8] iSd Internet Standard RFC 1918
[9] § 39 Abs. 5 BiBuG idgF

1.13 Art. 35

Die "Datenschutz-Folgenabschätzung" ist durchzuführen, wenn die Datenverarbeitung **voraussichtlich** ein **hohes** Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Die zu verabeitenden Daten basieren auf gesetzlichen Vorgaben. Ebenso gesetzlich verankert ist der Grundsatz der Gleichmäßigkeit der Abgabenerhebung[10], Es gehört mittlerweile zur ständigen Judikatur, daß diese Bestimmungen schwerer wiegen, als das Recht auf Datenschutz der Abgabenpflichtigen - auch wenn sich das Schutzrecht im Verfassungsrang befindet[11].

Da bereits der Gesetzgeber eine Eingriffsnorm geschaffen hat, die das Schutzniveau der Abgabenpflichtigen defininiert[12], darf ein vorausichtliches hohes Risiko für die Rechte und Freiheiten natürlicher Personen im allgemeinen verneint werden, wodurch die Durchführung einer Datenschutz-Folgenabschätzung entfallen kann.

Die oben zitierte Judikaturlinie bezieht sich auf das DSG 2000, das durch die EU-DSGVO, mit dessen Inkrafttreten am 25. Mai 2018, abgelöst wird. Die Zukunft wird zeigen, ob und gegebenenfalls wie, die ergangene Judikatur mit den Bestimmungen der EU-DSGVO aufrecht erhalten werden kann. Sollte es zu einer Revision der erwähnten ständigen Judikatur kommen, wird dieser Punkt zu überdenken bzw. zu überarbeiten sein.

1.14 Art. 37

Die "Benennung eines Datenschutzbeauftragten" ist nach Abs. 1 nicht nötig. Die BhB KG ist weder eine Behörde (lit. a), noch gehört es zur Kerntätigkeit eine regelmäßige bzw. systematische Überwachung von betroffenen Personen durchzuführen (lit. b). Ebensowenig gehört die umfangreiche Verarbeitung besonderer Kategorien (iSv sensibler Daten) von Daten zur Kerntätigkeit (lit. c).

Auf das Recht, nach Abs. 2, freiwillig einen Datenschutzbeauftragten zu ernennen, wird verzichtet. Somit entfällt auch die Mitteilungspflicht nach Abs. 7.

[10] stellvertretend für alle gleichartigen Bestimmungen: § 114 BAO
[11] Beispiel 1, Beispiel 2
[12] vgl. Art. 6 Abs. 1 lit. e

Kapitel 2

BiBuG

2.1 Vorbemerkungen

Die Berufsrechtnovelle BGBl I 135 / 2017 setzt im Wesentlichen im 2. Abschnitt (§§ 43 ff) die 4. EU-Geldwäsche-RL[1] zur Verhinderung der Geldwäsche und der Terrorismusfinanzierung um, indem einerseits das BiBuG novelliert wird und andererseits das WiEReG geschaffen wurde. Diese Novelle und das WiEReG sollten daher als Einheit gelesen werden.

Mit der BiBuG Novelle wird das bisherige starre Prüfschema durch einen risikobasierten Ansatz abgelöst. Dies bedeutet einerseits mehr Aufwand bei der Implementierung der nötigen Risikomanagement-Prozesse, andererseits darf erwartet werden, daß der risikobasierte Ansatz in der täglichen Praxis flexibler ist, als das alte starre Prüfungsschema.

Art. 33 der Richtlinie schreibt den Grundsatz "im Zweifel vernadern" vor, indem eine Meldepflicht statuiert wird, wenn der "Verdacht oder berechtigter Grund zu der Annahme" vorliegt oder "Kenntnis davon erhält", daß Gelder mit den zu bekämpfenden Vorgängen in Verbindung stehen.

Die von der Aufsichtsbehörde erlassene Bilanzbuchhaltungsberufe-Ausübungsrichtlinie 2017 (BB-AR 2017) ist anzwenden. Bei Kunden, für die ausschließlich die Personalverrechnung durchgeführt wird, kann nur eine Warnung bei vermuteter mißbräuchlicher (Schein)Anmeldung von Dienstnehmern ausgesprochen werden.

Soweit nicht durch das BiBuG oder den BB-AR vorgegeben, kommt der vom Fachverband UBIT herausgegebene Kurzleitfaden[2] zur Anwendung.

2.2 Risikobasierter Ansatz

Solange nur eine Person für die Kundenbuchhaltungen zuständig ist, kann der Aufbau der betriebsinternen risikobasierten Ausgestaltung der innerorganisatorischen Ausgestaltung entfallen.

[1] RL 849 / 2015 / EU
[2] Hier zu finden.

In das kundenbezogene Risikomanagement kann nur das einbezogen werden, was der Kunde freiwillig offenlegt. Ein Pflicht zur Offenlegung besteht nur gegenüber den Abgabenbehörden. Eventuell meldepflichtige Anomalien können nur anhand der Buchungsfälle feststellbar sein[3]. In einer Gesamtschau der bekannten Umstände und der zu beurteilenden Geschäftsfälle, unter Berücksichtigung des üblichen Geschäftsverlaufes[4], kann sich die Meldepflicht[5] einzelner Geschäftsfälle ergeben.

2.3 Sorgfaltspflichten

Diese werden von den §§ 45 ff BiBuG bzw. den §§ 14 ff BB-AR 2017 vorgegeben. Eine darüberhinaus gehende Dokumentation der verwendeten Strategien, Kontrollen und Verfahren fällt unter Betriebs- und Geschäftsgeheimnis und wäre an anderer Stelle zu dokumentieren.

Die Mitwirkung der BhB KG an Transaktionen beschränkt sich auf das Definieren der Zahlungen an die Abgabenbehörden im NetBanking des Kunden - unter der Voraussetzung, daß dies vom Kunden gewünscht wird. Die Prüfung und Freigabe dieser Zahlungen verbleibt beim Kunden.

Soweit nicht durch das BiBuG oder den BB-AR vorgegeben, kommen die vom Fachverband UBIT herausgegebenen Leifäden zur Annahme eines neuen Mandanten[6] bzw. der zur Verdachtsmeldung[7] zur Anwendung.

2.4 Aufbewahrungspflicht

Die im § 52c umgesetzte fünfjährige Aufbewahrungspflicht[8], ab dem Ende der Geschäftsbeziehung, ist kürzer als die vom Abgabenrecht normierte siebenjährige Aufbewahrungsfrist bzw. die vom § 18 Abs. 10 UStG definierten 22 Jahre. Wird allerdings bekannt, daß ein gerichtliches Strafverfahren durchgeführt wird, endet die Aufbewahrungpflicht frühestens fünf Jahre nach Beendigung des Verfahrens. Zu beachten ist weiters die (maximal) fünfjährige Verjährungsfrist der §§ 31 f FinStrG. Zur Anwendung kommt das späteste anzuwendende Datum für das Ende der Aufbewahrungsfrist nach Berücksichtigung obiger anzuwendender Vorschriften. Die allgemeine Verjährungsfrist von 30 Jahren des § 1478 ABGB kann somit überschritten werden.

[3] "faktengestützte Entscheidungsfindung" im Erw.Gr. 22 der RL 849/2015/EU.
[4] Siehe § 19 BB-AR 2017.
[5] In einer ex ante Beurteilung.
[6] Hier zu finden.
[7] Dieser hier.
[8] Art. 40 RL 849/2015/EU

Kapitel 3

WiEReG

3.1 Vorbemerkungen

Artikel 1 des BGBl I 136 / 2017 listet jene EU-Richtlinien auf, die das WiEReG umsetzt. Im Wesentlichen ist das die 4. Geldwäsche-RL zur Vermeidung von Geldwäsche und Terrorismusfinanzierung.

3.2 Rechte und Pflichten des Eigentümers

Da nicht jeder Rechtsträger automatisch auch der wirtschaftliche Eigentümer ist, haben sowohl der Rechtsträger (als juristische Person) als auch der wirtschaftliche Eigentümer (jene natürliche Person, die beherrschenden Einfluß auf die Tätigkeit des Rechtsträgers ausüben kann) Rechte und Pflichten iSd WiEReG.

3.2.1 Befreiung von der Meldepflicht

Als Kommanditgesellschaft ist die BhB KG gem. § 6 Abs. 1 von der Meldepflicht befreit, da alle Komplementäre natürliche Personen sind. Sollte es zu einer Änderung bei den Gesellschaftern kommen, wird eine Meldung nach § 5 Abs. 1 vorgenommen werden. Darüber hinaus kann die Richtigkeit der Daten in diesem Register jederzeit mittels Einsichtnahme in das Firmenbuch überprüft werden.

3.3 Die BhB KG als Verpflichteter

§ 9 Abs. 1 Z. 10 zählt die Berufsberechtigten gem. BiBuG zu den Verpflichteten, denen ebenfalls Rechte und Pflichten auferlegt sind.

3.3.1 Einsicht der Verpflichteten in das Register

Zu den Rechten gehört die Einsichtnahme in das Register der wirtschaftlichen Eigentümer - dazu wurden die Berufsrechte im BiBuG[1] entsprechend erweitert. Im Hinblick auf die BiBuG Novelle ist dies auch als Pflicht zu verstehen.

[1] § 2 Abs. Z. 8 bzw. § 3 Abs. 2 Z. 5 BiBuG

3.3.2 Sorgfaltspflichten der Verpflichteten gegenüber Kunden

§ 11 Abs. 1 verlangt u.a. als Sorgfaltspflicht gegenüber Kunden, daß nicht ausschließlich auf die im Register enthaltenen Daten vertraut werden darf. Die Verpflichteten haben nach einem risikobasierten Ansatz vorzugehen - dies deckt sich mit der berufsrechtlichen Anordnung des § 44 BiBuG.

Weiters normiert Abs. 3 eine Meldepflicht an das Register und Abs. 7 schließt deswegen eine Inanspruchnahme des Verpflichteten auf Schadenersatz aus. Dieser Ausschluß ergibt sich aus der Durchbrechung der Verschwiegenheitspflicht (§ 39 BiBuG) und der ausdrücklichen Anordnung im Art. 37 RL 849/2015/EU.

Die erläuternden Bemerkungen gehen davon aus, daß die Qualität der Daten im Register durch die, beim Verpflichteten zu implementierenden risikobasierten Prozesse, gesteigert werden kann und zu einer Entlastung der Nachforschungspflicht bei den Behörden führen wird. Womit der Verwaltungsaufwand und das Tragen des Risiko auf die Wirtschaftsteilnehmer abgewälzt wurde[2].

Die Praxis wird zeigen, ob die Erwartungen des Gesetzgebers, auf Entlastung der Behörden, in Erfüllung gehen werden.

3.3.3 Abgabenrechtliche Änderung

Durch die Verlagerung der Meldepflichten zu den Verpflichteten iSd WiEReG, wurde auch die Erhebungspflicht der Abgabenbehörde im § 115 Abs. 1 BAO entsprechend eingeschränkt und auf den Steuerpflichtigen überwälzt[3].

3.4 Strafbestimmungen

Diese sind im § 15 als reine Finanzordnungswidrigkeiten ausgestaltet, wobei Abs. 5 anordnet, daß diese niemals von einem Gericht zu ahnden sind. Dies ist notwendig, da die Strafen bis zu € 200.000,- betragen und die gerichtliche Zuständigkeit im FinStrG bei € 100.000,- beginnt - und somit dem ordentlichen Rechtsmittelverfahren entzogen wurden.

[2] "im Zweifel vernadern"

[3] "erhöhte Mitwirkungspflicht des Abgabenpflichtigen"